Open Enterprise Server 2018
Release Notes

November 2017

Legal Notices

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.microfocus.com/about/legal/.

Contents

About This Readme

Micro Focus Open Enterprise Server 2018 delivers all the enterprise-class networking, file, and print services that enterprises have relied on for years. OES 2018 is on SUSE Linux Enterprise 12 SP2, which provides valuable benefits including power savings, virtualization, manageability, and interoperability.

OES 2018 provides several new features that reduce administrative complexities and provide access to file and storage services regardless of eDirectory or Active Directory as an identity source. For information about the new features, see Chapter 1, "What's New or Changed in OES 2018," on page 7.

This Readme focuses on issues and information that are specific to the OES 2018 release.

Before installing this release, be sure to review the known issues, as described in "Service Issues" on page 17.

- Chapter 1, "What's New or Changed in OES 2018," on page 7
- Chapter 2, "Service Issues," on page 17
- Appendix A, "Deprecated Components and Services," on page 23

Use the following links to access the earlier versions of OES documentation:

- NetWare 6.5 SP8 Online Documentation website
- OES 2 SP3 Online Documentation website
- OES 11 Online Documentation website
- OES 2015 Online Documentation website

1 What's New or Changed in OES 2018

This section summarizes the new features introduced in Micro Focus Open Enterprise Server (OES) OES 2018 release and its patches.

1.1 What's New or Changed in Update 10 - OES 2018

Updated eDirectory and iManager

In this patch release on OES 2018, the eDirectory version is updated from eDirectory 9.1.3 to eDirectory 9.1.4 and the iManager version from iManager 3.1.3 to iManager 3.1.4.

NSS 64-bit ZID Support Enhancement

Beginning with this patch, NSS allows you to configure the ZID mode to ZID32 or ZID64 for local and shared volumes. It also provides an option to verify whether the volume is 64-bit ZID enabled or not.

For more information, see Setting and Viewing the ZID Mode for a Volume.

The `nss utility` has been enhanced to provide an option to force enable the ZID64 mode at a volume level. For more information, see nss /ForceVolumeZID64Mode=volumename.

IMPORTANT: When you access the NSS volume with ZID value greater than the 32-bit limit using AFP, users might experience abnormal behavior while performing the file operations on that volume because of Apple Filing Protocol (AFP) limitation. Therefore, administrators must ensure that AFP users have access to only those NSS volumes with ZID value less than the 32-bit limit. For more information, see AFP Known Issue in the Novell AFP for Linux Administration Guide.

DNS/DHCP Enhancement

DNS/DHCP Java Console now supports the OpenJDK versions 8,9,10,11,12 on Windows 7 SP1 and Windows 10.

DSfW Enhancement

DSfW now supports domain join and file access for NetApp Filer Ontap 9.1. To make use of it, you must update the OES 2018 DSfW server to this patch and then run the following script:

```
/opt/novell/xad/sbin/updateXadNmasMethods.pl
```

1.2   What's New or Changed in Update 7 - OES 2018

Updated eDirectory and iManager

In this patch release on OES 2018, the eDirectory version is updated from eDirectory 9.1 to eDirectory 9.1.3 and the iManager version from iManager 3.0.4 to iManager 3.1.3. eDirectory 9.1.x specific features can now be managed by this iManager, thus eliminating the limitation for using the standalone iManager 3.1 as per Update 3 - OES 2018 patch.

Folder Redirection Support

Folder Redirection allows users to redirect the path of a known folder to a network file share. Users can then interact with files in the redirected folder as if it still existed on the local drive. Beginning with this patch release, CIFS share can be enabled to host the redirected folders on the server. For information on configuring the CIFS share for Folder Redirection, see Enabling Folder Redirection Support (https://www.novell.com/documentation/open-enterprise-server-2018/file_cifs_lx/data/folder_redirection.html#folder_redirection).

1.3   What's New or Changed in Update 6 - iPrint

iprintman Enhancement

The following Print Manager enhancements are made to the iprintman command:

- **Redirecting a printer:** Sets a printer redirection. All the print jobs of one printer are redirected to another printer. To remove a printer redirect, do not specify the target printers.
- **Listing redirected printers:** Displays the list of redirected printers.

For more information, see Print Manager (PSM) Commands in the OES 2018 SP1: iPrint Administration Guide.

1.4   What's New or Changed in Update 6 - OES 2018

On applying this patch on the OES 2018 server, the Cloud Integrated Storage (CIS) agents (cis-agent.service, cis-recall-agent.service, and cis-scanner.service) are no longer supported and hence are stopped. These agents were installed as part of the NSS pattern.

These agents are stopped because with the release of OES 2018 SP1, CIS can be installed in a production environment and having the stale CIS (OES 2018) agents can impact the functionality of the OES server.

1.5   What's New or Changed in OES 2018 Post January 2019

Beginning with January 2019, the OES update repository and OES packages are signed with 4096 bit key. Therefore, during the process of new installation, upgrade, and update to OES 2018 post January 2019, you are prompted to import the new keys to the rpm keyring of the OES server. For more information, see Importing New Build Keys to the Keyring in the OES 2018: Installation Guide.

1.6 What's New or Changed in Update 4 - OES 2018

What's New or Changed in Domain Services for Windows (Update 4 - OES 2018)

Installation of Software Through GPO: The new installation of OES 2018 and upgrade from earlier OES versions to OES 2018 with the latest patch enables you to perform software installations through GPO.

On the existing OES 2018, to install software through GPO, an additional step of executing the script `software_gpo_setup.pl` is needed. For more information, see Group Policy Update Failure on Workstation When Installation of Software is Performed Through GPO in the OES 2018: Domain Services for Windows Administration Guide.

1.7 What's New or Changed in Update 3 - OES 2018 eDirectory 9.1

In this patch release on OES 2018, the eDirectory version is upgraded from eDirectory 9.0.3 to eDirectory 9.1 and the iManager version from iManager 3.0.3 to iManager 3.0.4.

If you are applying the patch while upgrading OES from its earlier version to OES 2018, the eDirectory schema is updated automatically.

If you are applying the patch on an existing OES 2018 server, you must manually extend the eDirectory schema by doing the following:

1. Install the OES 2018 Update 3 patches.
   - Update 3 - OES 2018 eDirectory 9.1 - Mandatory
   - Update 3 - OES 2018 - Recommended
2. Reboot the OES server.
3. In the terminal console, execute the command `ndsconfig upgrade` to extend the eDirectory schema.

iManager 3.1 is not a part of this patch release. To manage eDirectory 9.1 specific features from iManager, you must use the standalone iManager 3.1.

1.8 What's New or Changed in OES 2018

This section summarizes the new features and enhancements in Micro Focus Open Enterprise Server (OES) 2018 release.

1.8.1 Rebranding Changes

Novell is now part of Micro Focus. Products across the portfolio are now being rebranded to reflect Micro Focus or a more appropriate name. This corporate change impacts the name of products and components, user interfaces, logos, and so on. The product and documentation update to reflect these changes is being done in a phased manner.

As a result of this corporate change, the product name is now Micro Focus Open Enterprise Server. The new user interfaces, colors, and logos in OES 2018 gives a fresh look and feel to the product.

1.8.2 OES Installation

OES Install Media

Beginning with OES 2018, OES is installed only through OES Install Media, which is a single integrated install media that includes both SLES and OES. For more information on OES 2018 install procedure, see OES 2018: Installation Guide.

Traditional OES installation included both add-on install (SLES and OES as separate media) and integrated install media (a single media that includes both SLES and OES). The support for the add-on install is deprecated.

Channel Enhancement

Beginning with OES 2018, a single activation key of OES is sufficient to obtain all OES channels. SLES activation key is not required. OES activation key provide update channels for both SLES and OES.

All OES 2018 channels are available from NCC as earlier.

1.8.3 Novell Storage Services (NSS)

With OES 2018, NSS provides the following enhancements:

- **NSS 64-bit ZID Support:** NSS supports 64-bit IDs, which supports up to 8 trillion (8E12) ZIDs.

  NCP, CIFS, and FTP supports the NSS 64-bit ZID, which allows NSS to store up to 8 trillion files in a single volume. For more information, see ReZIDing Volumes in an NSS Pool in the OES 2018: NSS File System Administration Guide for Linux and OES 2018: NCP Server for Linux Administration Guide.

IMPORTANT: When the NSS volume is mapped through AFP, the NSS files and folders with ZIDs greater than 32-bit are not listed because of Apple Filing Protocol (AFP) limitation. If the NSS volume is shared over AFP, we recommend not to enable the 64-bit ZID option.

- **nss (Enhanced):** Beginning with OES 2018, the `nss` utility has been enhanced to support all the commands that `nsscon` utility supports.

  For more information, see nsscon in the OES 2018: NSS File System Administration Guide for Linux.

- **nsscon (Enhanced):** Commands are added for the following:

  - To update the SEV interval for eDirectory or AD.

  - To force the SEV update for eDirectory or AD users. Also, provided options to force the SEV update for a single eDirectory or AD user.

  For more information, see Security Equivalence Vector Update Commands in the OES 2018: NSS File System Administration Guide for Linux.

- To support the creation of pools, the following NSS tools have been enhanced:

  - **nssmu:** Beginning with OES 2018, the `nssmu` utility allows you to create only NSS64 pool type.

    For more information, see NSS Management Utility (NSSMU) Quick Reference in the OES 2018: NSS File System Administration Guide for Linux.

  - **iManager:** Beginning with OES 2018, the iManager storage plug-ins allows you to create only NSS64 pool type.

    For more information, see Creating a Pool in the OES 2018: NSS File System Administration Guide for Linux.

  - **NLVM:** Beginning with OES 2018, if you do not specify a type while creating a pool, NLVM defaults to NSS64 pool type. You can also create NSS32 pool type by providing the option NSS32.

    For more information, see Create Pool in the OES 2018: NLVM Reference.

- **Delayed Block Allocation:** This feature is now additionally available on volumes that are enabled with Compression and Quotas.

1.8.4   Common Internet File System (CIFS)

With OES 2018, CIFS provides the following enhancements:

- "SMB Enhancements" on page 11
- "Alternate Data Stream Support" on page 12
- "Dynamic Re-authentication Capability" on page 12
- "Utility to Convert AFP Metadata to CIFS Format" on page 12
- "Sever-Side Copy Support" on page 12
- "novcifs Command Changes" on page 12

SMB Enhancements

SMB v3 (SMB 3.0) Verb Compliance: Clients can now communicate with OES using the SMB 3.0 protocol.

SMB 3.0 has advantages of increased security achieved through using:

- Secure Dialect Negotiation
- AES-CMAC for signing
- SMB 3.0 encryption

In OES 2018, the default SMB protocol dialect is set to SMB 3.0.

Alternate Data Stream Support

Beginning with OES 2018, CIFS server supports Alternate Data Streams. To add customized metadata as extended attributes to the file or directory, enable alternate data stream on the server. This provides better performance.

Dynamic Re-authentication Capability

Beginning with OES 2018, the communication through SMB v2 is more secure with the implementation of dynamic re-authentication capability on the server. The session is expired based on the time out from the authentication protocol (Kerberos) and is re-authenticated from the client side.

Utility to Convert AFP Metadata to CIFS Format

On a Mac computer, if a customized color or icon is assigned to a file or folder on a volume mounted through AFP, then the customization is not visible when the same volume is mounted through CIFS. To enable the visibility of such customization, a new utility *migafp2cifs* is introduced that converts AFP specific metadata information to CIFS specific format. For more information on the options, see the migafp2cifs man page.

Sever-Side Copy Support

CIFS provides support for server-side copy operations. The CIFS clients can now off-load the copy operations to the CIFS server. This ensures improved file server performance because the network round-trip is avoided. By default, this feature is enabled on the CIFS server.

novcifs Command Changes

- **Alternate Data Stream:** You can enable or disable the data streams on the server.

    For more information, see Enabling or Disabling Alternate Data Stream in the OES 2018: Novell CIFS for Linux Administration Guide.

- **SMB v1 Disablement:** You can disable the SMB v1 sessions from the clients:

    For more information, see Disabling SMB v1 sessions in the OES 2018: Novell CIFS for Linux Administration Guide.

- **SMB 3.0 Encryption:** You can encrypt the client server sessions established at both global and share levels to protect data from corruption due to man-in-the-middle attacks:

    For more information, see Enabling or Disabling SMB 3.0 Encryption at Global Level, Enabling or Disabling SMB 3.0 Encryption at Share Level, and Enabling or Disabling Unencrypted Access to the Share in the OES 2018: Novell CIFS for Linux Administration Guide.

- **DNS Suffix:** You can set DNS suffix for the DFS referral target node server name.

    For more information, see Setting DNS Suffix in the OES 2018: Novell CIFS for Linux Administration Guide.

- **Display User Address:** You can enable or disable the updation of client IP address details for the logged in user in the eDirectory user object.

   For more information, see Updating Client IP Address Details in the OES 2018: Novell CIFS for Linux Administration Guide.

- **Log Level:** You can set the log level for the server to log messages.

   For more information, see Setting the Log Level in the OES 2018: Novell CIFS for Linux Administration Guide.

- **SMB Version Switching:** You can switch between SMB protocol versions. (The default for OES 2018 is SMB v3).

   For more information, see Toggling between SMB Versions in the OES 2018: Novell CIFS for Linux Administration Guide.

- **Deprecated Commands:** Beginning with OES 2018, the following command options are not available:

   - `novcifs [-b yes|no | --enable-debug=yes|no]`

   - `novcifs [-f yes|no | --enable-info=yes|no]`

   They are replaced by the new command `novcifs --log-level error | debug | info`.

1.8.5 Domain Services for Windows (DSfW)

With OES 2018, DSfW provides the following enhancements:

- "Schema Update" on page 13
- "Fine-Grained Password Policy" on page 13
- "AES Encryption" on page 13
- "NSS AD Member Server Support for DSfW" on page 14

Schema Update

DSfW on OES 2018 supports schema level and domain functional level equivalent to AD in Windows Server 2012. With updated schema level, the applications that integrates with the later releases of AD can work better in DSfW environment. This schema update is also on OES 2015 SP1 in patches. For more information, see Upgrading DSfW Environment to AD 2012 Level in the OES 2018: Domain Services for Windows Administration Guide.

Fine-Grained Password Policy

A feature supported on AD 2012 schema, enables user level configuration of password policies. Multiple password policies can be specified for a particular user and different restrictions can be applied to different set of users using this feature. For more information, see Fine-Grained Password Policy in the OES 2018: Domain Services for Windows Administration Guide.

AES Encryption

AES based encryption is a more secured encryption for communication between workstations and domain controllers when compared with the existing ARCFOUR based encryption. For more information, see Understanding AES Encryption for Communication in the OES 2018: Domain Services for Windows Administration Guide.

NSS AD Member Server Support for DSfW

OES NSS AD servers can now be configured as member servers to DSfW domain. DSfW domain users can access NSS AD file server using domain authentication.

1.8.6 Cloud Integrated Storage (CIS) (Technical Preview)

Cloud Integrated Storage is a hybrid cloud solution that provides a secure gateway to store, manage, and access data across the private or public cloud.

Highlights are:

- Helps reduce overall cost of ownership. Less frequently accessed data is placed on less expensive storage.
- Provides security and visibility of data that is stored on the cloud.
- Policy-based migration of data depending on last accessed time, file type, size, and so on.
- Users can always access the files irrespective of physical file location, local or cloud storage.

CIS is available with the OES 2018 ISO and focuses on managing your NSS data across cloud securely.

As a technical preview, the capability has not been tested for all use cases that traditional OES supports. It is recommended to pilot and test this component for your use case. If you want to use this component in a production or a non-test setup, refer to the CIS section in the OES 2018 EULA.

1.8.7 NetWare Core Protocol (NCP)

Support for 64-bit ZID NSS Files

In OES 2015 SP1 and earlier, NCP clients and other traditional applications can only work with 32-bit IDs, which support up to 4 billion (4E9) ZIDs. Therefore, NSS restricts ZIDs, and thus the number of files to the lower value.

Beginning with OES 2018, NCP supports salvage and purge operations on NSS files having 64-bit ZID number. To perform the salvage and purge of deleted files with 64-bit ZID number, you must use the following supported tool versions:

- Client for Open Enterprise Server 2 SP4 (IR7)
- Micro Focus iManager 3.0.3
- NetStorage

1.8.8 Password Expiry Notification

Beginning with OES 2018, password expiry notifications are introduced where the eDirectory users can change their password directly from the client device. A password expiry notification is displayed when you choose to map a network drive using CIFS, with the eDirectory credentials that is due to expire. It also provides the grace login information even after the password expires. For password expiry notification feature to be available on a workstation, the NFARM (OES File Access Rights Management) must be installed. For more information, see Password Expiry Notification on Windows in the OES 2018: Novell CIFS for Linux Administration Guide.

1.8.9 Salvage and Purge Support for Mac

The traditional Salvage and Purge operation can be done natively on Mac using NFARM (OES File Access Rights Management). For example, using NFARM installer for Mac, you can recover or permanently delete the files or folders that are already deleted.

For more information, see Salvage and Purge on Mac in the OES 2018: Novell CIFS for Linux Administration Guide.

1.8.10 iPrint for OES

iPrint for OES provides secured enterprise print services for your desktops, laptops, and mobile devices. iPrint integrates with your existing corporate printers, regardless of the printing vendor or brand allowing you to deliver self-service printer provisioning to your device users. The highlights are:

- Printing from your mobile devices made end-user easy
- Email print jobs to any Micro Focus iPrint printer
- WalkUp Printing
- Printing from Chromebook
- QuickPrint (Web Printing)
- iPrint Portal

For information on installation of iPrint for OES, see Installing and Configuring iPrint for OES.

1.8.11 OES Credential Store

To securely store proxy user credentials, OES 2018 introduces a new component named OES Credential Store (OCS).

In the versions earlier to OES 2018, the OES services supporting proxy users used CASA to store the proxy user credentials. CASA uses Mono as the runtime environment. However, OES 2018 is based on SLES 12 SP2, which does not support Mono as the runtime environment.

1.8.12 Systemd Changes

OES 2018 has moved to systemd, a new way of managing services. Both systemd and rcnovell command works for all the services. rcnovell commands get redirected and executes as systemd commands. However, if there are any redirection scripts that uses rcnovell start, stop, and status commands; ensure to modify the script with the appropriate systemd changes.

Systemd has replaced the traditional init scripts in OES 2018 and has introduced its own logging system called journal. The journal itself is a system service managed by systemd. It collects and stores logging data by maintaining structured indexed journals based on logging information received from the kernel, user processes, standard input and error of system services. The service messages are logged in `journalctl`. To view the service specific logs, use `journalctl -u <service>`. For example: `journalctl -u novell-tomcat`.

1.8.13 Supported Versions of Bundled Products

OES 2018 supports the following upgraded products bundled with OES:

- NetIQ eDirectory 9.0 SP3
- Micro Focus iManager 3.0 SP3

1.8.14 User Interface Enhancement

The install and upgrade work flow and user interface is changed in OES 2018 to provide you an enhanced install or upgrade experience. During install or upgrade, you are now provided with the information on components and entitlements of OES in the form of slide show.

The interface of OES Remote Manager (NRM) is refreshed to provide a new and modern look.

1.8.15 iFolder

iFolder capabilities are now provided by Micro Focus Filr. Filr has been designed to provide a less administrative and more secure file synchronization capabilities. OES customers are entitled to Filr Standard. For more information on Filr, see Micro Focus Product Site. Beginning with OES 2018, iFolder is no longer a part of OES.

1.8.16 Samba

Novell-Samba service pattern is being deprecated and will not be supported in future OES releases.

1.8.17 Unchanged Components in OES 2018

Besides bug fixes, there are no other changes to the following components for OES 2018:

- Apple Filing Protocol (AFP)
- Distributed File Services (DFS)
- Dynamic Storage Technology (DST)
- Linux User Management (LUM)
- Migration Tool
- Novell Cluster Services
- Novell FTP
- Novell Identity Translator (NIT)
- Linux Volume Manager (NLVM)
- OES User Rights management (NURM)
- Storage Management Services (SMS)

2 Service Issues

This section documents the known issues in Open Enterprise Server 2018 (OES 2018).

Additional tips are found in the troubleshooting sections of the OES service administration guides.

2.1 OES Installation or Upgrade

2.1.1 Registering to Update Channel Post Upgrading to OES 2018 and then Applying the Patches Displays a Conflict Warning

When a fully patched OES 2015 SP1 server is upgraded to OES 2018 and registered to the update channel post upgrade, a conflict message is displayed during patching the server at a later time. This issue is not observed if the patches are applied during the upgrade process.

2.1.2 Ignore the Nessus Scan Critical Vulnerability Error on OES Server for SLES 12 SP2

The error is:

```
The Unix operating system (SLES 12 SP2) running on the remote host is no longer
supported. Lack of support implies that no new security patches for the product
will be released by the vendor. As a result, it is likely to contain security
vulnerabilities.
```

OES 2018 is an integrated media that includes both SLES 12 SP2 and OES 2018. All the SLES 12 SP2 patches that are necessary for running the OES services securely and with stability are made available via the OES 2018 update channels. So, even if SLES 12 SP2 is out of General Support, it does not impact the OES customers.

You can safely ignore the Security Vulnerability error given by the Nessus Scan report as it does not consider that SLES 12 SP2 is in Long Term Service Pack Support (LTSS) with the OES customers. We take security and stability of the OES servers seriously and we know they are a priority for our customers and hence are a priority for us too.

2.1.3 NICI SDI Key "w0" Object Issue

If the NICI SDI key object "w0" (w in lowercase) is present in the Security container of a tree and OES 2018 server is added to the same tree, it automatically creates a NICI AES 256 bit tree key. However, OES does not support the NICI AES 256 bit tree key.

The following are the scenarios:

◆ **Case 1:** If the tree contains the "w0" (w in lowercase) object and no OES 2018 server is added to the tree.

Before adding OES 2018 server to the tree, rename the NICI SDI key object "w0" (w in lowercase) to "W0" (W in uppercase) using iManager.

1. Log in to iManager as Admin.
2. Go to **Objects** and select **Tree**.
3. Click **<Tree_name> > Security > KAP**.
4. Select the "w0" object. Click the **Actions** tab and select **Rename Object**.
5. Specify the new object name as W0 (W in uppercase) and click **OK**.

◆ **Case 2:** If you have already added OES 2018 server to the tree that contains the "w0" (w in lowercase) object.

In this case, contact Micro Focus Technical Support for further guidance.

2.2 Apple Filing Protocol (AFP)

2.2.1 AFP Does Not Support NSS Volumes With ZID Value Greater Than the 32-bit Limit

On Mac, when you access the NSS volumes with ZID value greater than the 32-bit limit, AFP users might experience abnormal behavior while performing the file operations on that volume. For more information, see AFP Known Issue in the Novell AFP for Linux Administration Guide.

2.3 Cluster Services (NCS)

2.3.1 iSCSI Service Might Not Start After Upgrade to OES 2018

iSCSI service is disabled by default on SLES 12 SP2. Because of iSCSI start failure, NCS might not come up after upgrade. Ensure iSCSI service is up and enabled before starting NCS service.

2.4 Common Internet File System (CIFS)

2.4.1 Folder Redirection to an OES CIFS Share Is Not Supported

Folder Redirection of a user's folders to a CIFS share on an OES server is currently not supported.

2.5 DNS/DHCP Services

2.5.1 DHCP Pattern Conflict

When you select DHCP pattern post installation, a pattern conflict message is displayed. To continue, select the first option.

2.6 Domain Services for Windows (DSfW)

2.6.1 DSfW Specific Configuration Loss on Upgrading a DSfW Server to OES 2018 and Applying the Patch Update 9 - OES 2018 or later

During upgrade to OES 2018, the `smb.conf` file is not updated with the DSfW specific configuration from OES 2015 SP1 server. Because of this, after upgrade to OES 2018 with patch level Update 9 or later, the `smb.conf.oes2018-upgrade-save` file does not include the DSfW specific configuration. To resolve this issue, take a backup of the `smb.conf` file before the upgrade and after the upgrade, replace the files `/etc/samba/smb.conf` and `smb.conf.oes2018-upgrade-save` with the backed up `smb.conf` file. This avoids failure of DSfW functionalities like GPO and samba share access.

2.6.2 Transfer and Seize of Roles From One DC to Another in a Domain Fails

PDC role transferring and seizing operation fails in the step of executing the script `UpdatePDCMaster.pl` because of an issue with perl DNS resolver.

2.6.3 User Creation Fails from Windows 8.1 and Windows 10

For a Windows 8.1 or Windows 10 workstation that is joined to a DSfW domain, user creation fails with an error message.

2.6.4 DSfW Interoperability Issues

> **IMPORTANT:** The following list is provided for your convenience. Do not consider the list as complete. Be sure to consult the documentation for your other Micro Focus products for information on interoperability issues with DSfW.

ZENworks Endpoint Security Management 3.5

On an OES 2018 server with DSfW installed, the Endpoint Security Management utility fails on all DSfW server ports.

Micro Focus has no current plans to change this.

2.6.5 Mac El Capitan (10.11.1 and later) Fails to Join a DSfW Domain

A Mac El Capitan (10.11.1 and later) fails to join a DSfW domain, due to schema update issues.

2.7 eDirectory

The following are the known OES-specific eDirectory issues. For general eDirectory issues, refer to the eDirectory documentation website.

2.7.1 eDirectory Features Not Supported in OES 2018

With OES 2018, the following eDirectory features are not supported:

- Creation of AES 128-bit tree key or 256-bit tree key
- SUITE B

  For more information, see Configuring eDirectory in Suite B Mode in the NetIQ eDirectory Administration Guide.
- Enhanced Background Authentication (EBA)
- FIPS

2.7.2 eDirectory Not Restarting Automatically

After a system crash or power failure, eDirectory services (`ndsd`) might not automatically start in some situations.

To start eDirectory again:

1 Delete the `/var/opt/novell/eDirectory/data/ndsd.pid` file.
2 At a terminal prompt, enter `systemctl start ndsd.service`

2.8 Linux User Management (LUM)

◆

2.8.1 Special Characters in Container Name is Not Supported

LUM service configuration fails if the container name contains special characters \, *, (,),= and space.

2.9 Migration Tool

2.9.1 Migration to OES 2018

Trustee migration across different tree is not working.

2.10 NetStorage

2.10.1 NetStorage Service Configuration Fails

NetStorage service configuration fails if the container name contains special characters `(`, `)`, and space.

2.11 Novell FTP

2.11.1 File Upload to DFS Junction Fails

AD users are unable to upload files to the DFS Junction.

2.12 Novell Storage Services (NSS)

◆
◆
◆

2.12.1 Support for Mixed Cluster Nodes and NSS Active Directory Media Upgrades

In a mixed node cluster environment, before upgrading the NSS media to support Active Directory users or creating 64-bit pools, it is strongly recommended that you upgrade all the nodes to OES 2015 or later. This is because the upgraded NSS resources might not be accessible from cluster nodes that are not upgraded to OES 2015 or later.

2.12.2 Support for Mixed Cluster Nodes and NSS Trustee Index Media Upgrades

In a mixed node cluster environment, before upgrading the NSS media to support Trustee Index, it is strongly recommended that you upgrade all the nodes to OES 2015 SP1 or later. This is because the upgraded NSS resources might not be accessible from cluster nodes that are not upgraded to OES 2015 SP1 or later.

2.12.3 RAID 5 Issues

Some issues can occur when you lose a device in an NSS software RAID 5 device, or when you expand an NSS software RAID 5 device. The following issues happen intermittently:

When a segment is missing in an NSS RAID 5 because of a device failure, the pool might hang until the device driver reports the error, and then the RAID continues. The hang time depends on the underlying device driver timeout conditions. For iSCSI devices, this includes iSCSI driver timeout. For extended hangs, the pool might also get deactivated.

2.13 SLES Modules and Extensions

2.13.1 Unavailability of SLES Modules and Extension in OES 2018 Update Channel

All the SLES modules and extensions are not included in OES 2018. On upgrading to OES 2018, only Containers module of SLES is available in the OES 2018 Update Channel. Few of the other modules are being considered for inclusion in the upcoming releases. For example, Web and Scripting module.

A Deprecated Components and Services

- Beginning with OES 2018, iFolder is not included. New installations of OES 2018 will not include patterns to install iFolder.

- Beginning with OES 2015, Archive and Version Services (AV) and QuickFinder services are not included. New installations or upgrade to OES 2015 and later will not include patterns to install these components.

  If you are upgrading to OES 2018 from an OES 11 SP3 or earlier server that includes the Archive and Versioning Services (AV), QuickFinder, and iFolder packages, these packages and the associated data will not be accessible on the OES 2018 server. However, the iManager plug-ins for AV, QuickFinder, and iFolder are still available post upgrade, and you can use them to manage servers prior to OES 2015.

- Beginning with OES 11 SP2, no further functional enhancements are planned for NetStorage. For more information, see the Notice about certain OES services.